DETAILED ACTION

1. This action is responsive to communication filed on 8/11/2011. Claims 1-4,6-8,10-15,17-27 are subject to examination. Claims 26-27 are newly added claims. Claims 5,9 and 16 are cancelled.
2. This amendment has been fully considered and entered.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 1/2/2012 has been entered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4,6-8,10-15,17-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koskimies et al. U.S. Patent Publication # 2004/0081110 (hereinafter Koskimies) in view of Paatero et al. U.S. Patent Publication # 2004/0176068 (hereinafter Paatero)

As per claim 1, Koskimies teaches a computer device (having wireless communication capability, comprising:

-a wireless communication portal for selectively sending and receiving data across a wireless network (Paragraph 50, 52, 66); **NOTE:** The reference teaches having a WAP page of the sound download service at the content server which has midlets (i.e. sending/receiving data) and downloading a midlet across the network through infrared or Bluetooth functionality.

-a computer platform (Fig. 1 element 110) including a resident application environment and selectively download applications to the computer platform (Paragraph 50, 56, 59) the resident application environment configured to selectively download application through the portal (Paragraph 50,56) that comply with a predefined security protocol (Paragraph 78,79,80); **NOTE:** The reference teaches having mobile device (computer platform) which includes java "mobile information device applets (midlets)" which are downloaded through a WAP page of the sound download service (i.e. portal page). In Paragraph 59, it states selecting one or multiple midlets by the user to download at the mobile device (selectively download applications). In Paragraph 78, 79, 80, it teaches that downloading can be done by encrypting before downloading and decrypting by a particular target (i.e. comply with a predefined security protocol). According the specification of the current invention, it states applications are midlets or applets. Therefore, Koskimies teaches midlets/applets.

-a data store (i.e. content server or storage on the mobile device) in communication with the computer platform and selectively sending data to and receiving

data from the computer platform (Paragraph 50, 53); **NOTE:** The reference teaches midlet will retrieve a list of available content items from the content server (i.e. data store) which is in communication with the mobile device. After selecting a content item (i.e. sound clip), the midlet can effect charging such as by sending an SMS and can then download the content and immediately forward it to the limited device (selectively sending data to and receiving data from the computer platform).

- a download manager resident on the computer platform that at least selectively downloads applications through the portal that do not comply with the predefined security protocol (Paragraph 78, 83) **NOTE:** The reference states downloading content to a device unauthorized by the content creator, and downloading unauthorized content (i.e. unauthorized by the device maker) to the device i.e. downloading application that does not comply with the security protocol.

wherein the selectively downloaded applications that comply with the predefined security protocol are executed by the computer platform within the resident application environment (Paragraph 50, 59) NOTE: The reference teaches that the midlet is downloaded to the mobile device, the user can select one of the midlets via the mobile device and midlet is executed in the mobile device.

Koskimies does not teach wherein the selectively downloaded applications that do not comply with the predefined security protocol are executed by the download manager outside of the resident application environment.

Paatero particularly points out a download manager resident on the computer platform that at least selectively downloads applications that do not comply with the

predefined security protocol (Paragraph 26) and wherein the selectively downloaded applications that do not comply with the predefined security protocol are executed by the download manager outside of the resident application environment. (Paragraph 13, 27-28). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Paatero's teaching Koskimies's teaching to come up with downloading and executing application which does not comply with security protocol. The motivation for doing so would be sometimes downloading application which does not comply with security protocol are safe, therefore there is no harm to the user's computer in downloading them.

As per claim 2, Koskimies and Paatero teaches the device of claim 1, but Koskimies further teaches wherein the download manager (i.e. sound download service on the WAP page) exists within resident application environment and uses an existing application download interface (Paragraph 50, 66).

As per claim 3, Koskimies and Paatero teaches the device of claim 1, but Paatero further teaches wherein the wherein the download manager further manages executing the downloaded application that does not comply with the predefined security protocol is immediately executed (Paragraph 28).

As per claim 4, Koskimies and Paatero teaches the device of claim 1, but Koskimies further teaches wherein a downloaded application that does not comply with the predefined security protocol is stored (Paragraph 78, 83), and but Koskimies fails to teach the stored application is executed through the download manager. Paatero teaches the stored application is executed through the download manager (Paragraph

26-28). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Paatero 's teaching in Koskimies's teaching to come up with executing the application through download manager. The motivation for doing so would to test/verify the application by executing whether it is safe or malicious.

As per claim 6, Koskimies and Paatero teaches the device of claim 1, but Koskimies also teaches wherein the download manager further manages storage of the selectively downloaded application that do not comply with the predefined security protocol in the data store (Paragraph 83)

As per claim 7, Koskimies and Paatero teaches the device of claim 1, but Paatero further teaches wherein the predefined security protocol is verifying the origination of a given application to be downloaded (Paragraph 28-29).

As per claim 8, Koskimies and Paatero teaches the device of claim 1, but Paatero further teach wherein the predefined security protocol is verifying the presence of a certificate within a given application to be downloaded (Paragraph 28-30). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Paatero's teaching in Koskimies's teaching to come up with verifying the presence of certificate within a given application to be downloaded. The motivation for doing so would be to verify the identity of the application/file and make sure the it is safe/legit/virus-free, thereby the certificate provides a safe/virus-free certificate.

As per claim 10, Koskimies teaches a computer device having wireless communication capability, comprising: a wireless communication means for selectively sending and receiving data across a wireless network (Paragraph 50, 52, 66); **NOTE:** The reference teaches having a WAP page of the sound download service at the content server which has midlets (i.e. sending/receiving data) and downloading a midlet across the network through infrared or Bluetooth functionality.

a computer means selectively downloading applications, the computer means configured to selectively download application (Paragraph 50,56) through the wireless communication means that comply with a predefined security protocol (Paragraph 78,79,80); **NOTE:** The reference teaches having mobile device (computer platform) which includes java "mobile information device applets (midlets)" which are downloaded through a WAP page of the sound download service (i.e. portal page). In Paragraph 78, 79, 80, it teaches that downloading can be done by encrypting before downloading and decrypting by a particular target (i.e. comply with a predefined security protocol). According the specification of the current invention, it states applications are midlets or applets. Therefore, Koskimies teaches midlets/applets.

-a means for selectively downloading application through the wireless communications means that do not comply with the predefined security protocol (Paragraph 50, 78, 83) **NOTE:** The reference states downloading content to a device unauthorized by the content creator, and downloading unauthorized content (i.e. unauthorized by the device maker) to the device i.e. downloading application that does

not comply with the security protocol. The downloading is done on the phone using infrared or Bluetooth communication (i.e. wireless communication)

wherein the selectively downloaded applications that comply with the predefined security protocol are executed by the computer platform within the resident application environment (Paragraph 50, 59) NOTE: The reference teaches that the midlet is downloaded to the mobile device, the user can select one of the midlets via the mobile device and midlet is executed in the mobile device.

Koskimies does not teach wherein the selectively downloaded applications that do not comply with the predefined security protocol are executed by the download manager outside of the resident application environment.

Paatero particularly points out a download manager resident on the computer platform that at least selectively downloads applications that do not comply with the predefined security protocol (Paragraph 26) and wherein the selectively downloaded applications that do not comply with the predefined security protocol are executed by the download manager outside of the resident application environment. (Paragraph 13, 27-28). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Paatero's teaching Koskimies's teaching to come up with downloading and executing application which does not comply with security protocol. The motivation for doing so would be sometimes downloading application which does not comply with security protocol are safe, therefore there is no harm to the user's computer in downloading them.

As per claim 11, Koskimies teaches a method of selectively downloading through a wireless connection to a computer device, comprising the steps of: downloading from the wireless connection to the computer platform of the computer device an application that does not comply with a predefined security protocol for use at that computer device (Paragraph 50, 78, 83) **NOTE:** The reference states downloading content to a device unauthorized by the content creator, and downloading unauthorized content (i.e. unauthorized by the device maker) to the device i.e. downloading application that does not comply with the security protocol. The downloading is done on the phone using infrared or Bluetooth communication (i.e. wireless communication)

-the computer platform including a resident application environment for downloading applications utilizing a predefined security protocol for at least downloading an application (Paragraph 50, 53, 59), the downloading of the non-complying application occurring through the use of a download manager resident on the computer platform; (Paragraph 78, 83) and for executing applications downloaded in compliance with the predefined security protocol within the resident application environment(Paragraph 50, 59) **NOTE:** The reference teaches having mobile device (computer platform) which includes java “mobile information device applets (midlets)” which are downloaded through a WAP page of the sound download service (i.e. portal page). In Paragraph 59, it states selecting one or multiple midlets by the user to download at the mobile device (selectively download applications). In Paragraph 78, 79, 80, it teaches that downloading can be done by encrypting before downloading and decrypting by a particular target (i.e. comply with a predefined security protocol).

According the specification of the current invention, it states applications are midlets or applets. Therefore, Koskimies teaches midlets/applets. The reference teaches that the midlet is downloaded to the mobile device, the user can select one of the midlets via the mobile device and midlet is executed in the mobile device.

Although Koskimies teaches an application that does not comply with a predefined security protocol (Paragraph 78, 83), But Koskimies does not teach executing the non-complying application at the computer device with the download manager outside of the resident application environment. Paatero teaches the downloading of the non-complying application occurring through the use of a download manager resident on the computer platform (Paragraph 26) executing the non-complying application at the computer device with the download manager outside of the resident application environment (Paragraph 13, 27-28). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Paatero's teaching gin Koskimies's teaching to come up with downloading application which does not comply with security protocol. The motivation for doing so would be sometimes downloading application which does not comply with security protocol are safe, therefore there is no harm to the user's computer in downloading them

As per claim 12, Koskimies and Paatero teaches the method of claim 11, but Koskimies further teaches wherein the download manager (i.e. sound download service on the WAP page) exists within resident application environment and the step of downloading uses an existing application download interface (Paragraph 50, 66).

As per claim 13, Koskimies and Paatero teaches the method of claim 11, but Paatero further teaches further comprising the steps of: storing, with the download manager the non-complying application (Paragraph 27-28) and executing the stored application through the download manager (Paragraph 28). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Paatero's teaching in Koskimies's teaching to come up with executing the application through download manager. The motivation for doing so would to test/verify the application by executing whether it is safe or malicious.

As per claim 14, Koskimies and Paatero teaches the method of claim 11, but Paatero further teaches further comprising the step of verifying whether the non-complying application complies with the predefined security protocol (Paragraph 28-30)

As per claim 15, Koskimies and Paatero teaches the method of claim 14, but Paatero further teach wherein the step of verifying includes verifying the presence or absence of a certificate within the non-complying application (Paragraph 28-30). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Paatero's teaching in Koskimies's teaching to come up with verifying the presence of certificate within a given application to be downloaded. The motivation for doing so would be to verify the identity of the application/file and make sure the it is safe/legit/virus-free, thereby the certificate provides a safe/virus-free certificate.

As per claim 17, Koskimies and Paatero teaches the method of claim 11, but Paatero further teaches further comprising the step of downloading the download

manager to the computer platform of the computer device after a request to download the non-complying application has been made (Paragraph 24), and prior to the step of downloading the non-complying application (Paragraph 26-27).

As per claim 18, Koskimies teaches a method of selectively downloading through a wireless connection to a computer device comprising the steps of: a step for downloading through the wireless communication to the computer platform of the computer device an application that does not comply with a predefined security protocol for use within a resident application environment at that computer device (Paragraph 50, 78, 83) **NOTE:** The reference states downloading content to a device unauthorized by the content creator, and downloading unauthorized content (i.e. unauthorized by the device maker) to the device i.e. downloading application that does not comply with the security protocol. The downloading is done on the phone using infrared or Bluetooth communication (i.e. wireless communication)

-a step for executing the downloaded application at the computer device outside of the resident application environment (Paragraph 78, 83).

-wherein application that comply with the pre-defined security protocol are configured for execution within the resident application environment (Paragraph 50, 59) NOTE: The reference teaches that the midlet is downloaded to the mobile device, the user can select one of the midlets via the mobile device and midlet is executed in the mobile device.

Although Koskimies teaches downloading through the wireless communication to a computer platform of the computer device an application that does not comply with a

predefined security protocol for use within a resident application environment at that computer device but Paatero further teaches downloading to a computer platform of the computer device an application that does not comply with a predefined security protocol for use within a resident application environment at that computer device (Paragraph 26-27). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Paatero's teaching gin Koskimies's teaching to come up with downloading application which does not comply with security protocol. The motivation for doing so would be sometimes downloading application which does not comply with security protocol are safe, therefore there is no harm to the user's computer in downloading them.

As per claim 19, it teaches same limitation as claim 11, therefore rejected under same basis.

As per claim 20, Koskimies and Paatero teaches the non-transitory computer-readable medium of claim 19, but Koskimies further teaches wherein the download manager (i.e. sound download service on the WAP page) is resident on the computer platform (Paragraph 50)

As per claim 21, Koskimies and Paatero teaches the non-transitory computer-readable medium of claim 19, but Paatero further teaches wherein the download manager is loaded to the computer platform after a request to download of the non-complying application (Paragraph 24) and prior to download thereof (Paragraph 26-27)

As per claim 22, Koskimies and Paatero teaches the computer device of claim 1, but Koskimies further teaches wherein the download manager exists within resident

application environment and uses an existing application download interface (Paragraph 50, 56)

As per claim 23, Koskimies and Paatero teaches the computer device of claim 1, but Koskimies further teaches wherein the pre-defined security protocol includes an application validation requirement of the resident application environment (Paragraph 79-81)

As per claim 24, Koskimies and Paatero teaches the computer device of claim 1, but Koskimies further teaches wherein the application being downloaded by the resident application environment in compliance with the pre-defined security protocol (Paragraph 79-81) and the application being downloaded by the download manager in non-compliance with the pre-defined security protocol are both stored in the data store (Paragraph 78, 83).

As per claim 25, Koskimies and Paatero teaches the computer device of claim 1, but Paatero further teach wherein the predefined security protocol is configured to protect the computer device (Paragraph 28-30). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Paatero's teaching in Koskimies's teaching to come up with protecting the computer. The motivation for doing so would be to so the computer/device does not receive any virus/unsafe application/program loaded into the computer.

As per claim 26, Koskimies and Paatero teaches the computer device of claim 1, but Paatero further teach wherein the compliance with the pre-defined security protocol

for a given application is based upon information contained with the given application during download and prior to execution of the given application (Paragraph 13, 28-30)

As per claim 26, Koskimies and Paatero teaches the computer device of claim 1, but Koskimies further teach wherein the resident application environment is requested to download a given application (Paragraph 50, 59, 78, 83). Koskimies does not teach wherein the resident application environment refuses to download the given application based on the given application failing to comply with the pre-defined security protocol, wherein the download manager is subsequently requested to download the given application after the refusal, wherein the download manager downloads the given application responsive to the subsequent request.

Paatero teach wherein the resident application environment refuses to download the given application based on the given application failing to comply with the pre-defined security protocol (Paragraph 13, 27-28), wherein the download manager is subsequently requested to download the given application after the refusal (Paragraph 13, 28), wherein the download manager downloads the given application responsive to the subsequent request (Paragraph 25,28-30). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Paatero's teaching in Koskimies's teaching to come up with having refusing to download un-complied application, download the application after the refusal and the request. The motivation for doing so would because the application is important to the user, therefore user wants to download regardless of application being unsecure and downloading the application manually through the download manager.

Response to Arguments

Applicant's arguments with respect to claims 1-4,6-15,17-27 and Bilange and Hericourt reference have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

   A). Kiessling et al. U.S. Patent # 6,901,251

   B). Stillerman et al. U.S. patent # 7,467,417

4. A shortened statutory period for response to this action is set to expire **3 (three) months and 0 (zero) days** from the mail date of this letter. Failure to respond within the period for response will result in **ABANDONMENT** of the applicant (see 35 U.S.C 133, M.P.E.P 710.02, 710.02(b)).

5.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dhairya A. Patel whose telephone number is 571-272-5809. The examiner can normally be reached on Monday-Friday 8:00AM-5: 30PM, first Fridays OFF.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee can be reached on 571-272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DAP

/DHAIRYA A PATEL/

Examiner, Art Unit 2451